UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/964,272	09/25/2001	Michael P. Lyle	RECOP018	9955

21912 7590 03/28/2005

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 03/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/964,272	LYLE ET AL.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 September 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 September 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *02122002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 are pending.

Drawings

2. The informal drawings are not of sufficient quality to permit examination. Accordingly, replacement drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to this Office action. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action.

Applicant is given a TWO MONTH time period to submit new drawings in compliance with 37 CFR 1.81. Extensions of time may be obtained under the provisions of 37 CFR 1.136(a). Failure to timely submit replacement drawing sheets will result in ABANDONMENT of the application.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-2, 10-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over I'Anson et al (EPO 0474932) and further in view of Shanklin et al (US 6487666).

As per claims 1, and 19-21, I'Anson discloses identifying at least two states associated with the network protocol in which a first host system communicating with a second host system using the network protocol may be placed; defining at least one valid transition between a first state of the at least two states and a second state of the at least two states (see p. 4 lines 27-49).

I'Anson fails to disclose expressing the at least one valid transition in the form of a regular expression and using the regular expression to analyze the network protocol stream.

However, Shanklin et al teaches the use of regular expressions (see column 6 lines 39-57).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Shanklin et al's regular expressions to analyze the protocol of I'Anson.

Motivation to do so would have been to recognize and evaluate identifiers, special symbols, or other tokens.

As per claim 2, the modified I'Anson and Shanklin et al system discloses using the regular expression to analyze the network protocol stream comprises compiling the regular expression into computer code (see column 6 lines 39-57).

As per claims 10-11, the modified I'Anson and Shanklin et al system discloses keeping track of which of the at least two states the first host system currently is in and changing the tracked state of the first host system from the first of the at least two states to the second of the at least two states in the event the analysis of the network protocol stream indicates the at least one valid transition has taken place (see p. 4 lines 27-49).

As per claims 12 and 18, the modified I'Anson and Shanklin et al system discloses defining at least one invalid operation for the first host system in at least one of the at least two states; expressing the at least one invalid operation as a second regular expression; and using the second regular expression to analyze the network protocol stream (see page 4).

As per claims 13-14, the modified I'Anson and Shanklin et al system discloses the invalid operation may indicate that a security-related event has taken or is taking place and defining

a further state corresponding to the invalid operation (see p. 4 lines 18-26 where the security related event is the intrusion of Shanklin et al).

As per claims 15-17, the modified I'Anson and Shanklin et al system discloses keeping track of which state, from the set comprising the at least two states and the further state, the first host system currently is in; and changing the state of the first host system to the further state in the event that the analysis of the network protocol stream indicates the invalid operation has taken place and in the event that the analysis of the network protocol stream indicates the invalid operation has taken place, an indication that the invalid operation has taken place then discontinuing analysis of the network protocol stream once the state of the first host system has been changed to the further state (see page 4).

5. Claims 3-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified I'Anson and Shanklin et al system as applied to claim 2 above, and further in view of Wijendran (AWK-to-C Translator).

As per claims 3-4, the modified I'Anson and Shanklin et al system fails to disclose the use of optimal C programming language code.

However, Wijendran teaches this optical C code (see page 1).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Wijendran's optical C code in the modified I'Anson and Shanklin et al system.

Motivation to do so would have been to maximize runtime performance (see page 1).

6. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified I'Anson and Shanklin et al system as applied to claim 2 above, and further in view of Mangione-Smith (How many vector registers are useful?).

As per claim 5, the modified I'Anson and Shanklin et al system fails to disclose the use of nearly optimal computer code.

However, Mangione-Smith teaches nearly optical code (see page 1).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Mangione-Smith's nearly optical code in the modified I'Anson and Shanklin et al system.

Motivation to do so would have been that nearly optimal code requires less vector registers (see page 1).

7. Claims 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified I'Anson and Shanklin et al system as applied to claim 1 above, and further in view of Blam (US 6467041).

As per claim 6, the modified I'Anson and Shanklin et al system fails to disclose copying the stream to a third party to be analyzed.

However, Blam teaches a third party analyzer (see column 6 lines 5-29).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Blam's third party analyzer to analyze the protocol analyzer of the modified I'Anson and Shanklin et al system.

Motivation to do so would have been to perform the analysis regardless of what resources are on the network or client (see column 6 lines 5-29).

As per claims 7-9, the modified I'Anson, Shanklin et al and Blam system discloses the network protocol stream comprises packets of data, each packet being associated with a sequence number indicating its position relative to other packets in the protocol stream, and the third system reassembles the packets into the order indicated by the respective sequence numbers of the packets received where a copy of the network protocol stream

is maintained in the third system until analysis has been completed and in the event the packets are received by the third system in sequence number order, a copy is maintained in the third system only of those packets comprising the portion of the network protocol currently under analysis (see I'Anson pages 4-5 and Blam column 6 lines 5-29).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Bernhard et al (US 6609205) discloses detecting network intrusions using regular expressions, Shaffer et al (US 6122743) discloses a third party analyzer, and Dietz et al (US 6665725) disclose a network protocol analyzer.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

MJP

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER